aurigin

Document Summary

New Search Help

Preview Claims
Preview Full Text
Preview Full Image

Email Link:

Document ID:	JP 11-161618 A2
Title:	MOBILE COMPUTER MANAGEMENT DEVICE, MOBILE COMPUTER DEVICE, AND MOBILE COMPUTER REGISTERING METHOD
Assignee:	TOSHIBA CORP
Inventor:	INOUE ATSUSHI ISHIYAMA MASAHIRO FUKUMOTO ATSUSHI TSUDA YOSHIYUKI OKAMOTO TOSHIO
US Class:	
Int'l Class:	G06F 15/16 A; G06F 13/00 B; G06F 15/00 B; H04L 09/32 B; H04L 12/46 B; H04L 12/28 B; H04L 12/66 B
Issue Date:	06/18/1999
Filing Date:	09/03/1998

Abstract:

PROBLEM TO BE SOLVED: To provide the mobile computer management device (home agent) which can authenticate a user who is operating a mobile computer when the mobile computer sends a registration message of its current position to the mobile computer management device from its movement destination network.

SOLUTION: The mobile computer management device which is installed in the home network of the mobile computer 2 and enables the mobile computer 2 to have a communication by moving among networks 1a to 1c has a registering function which registers information on the current position of the mobile computer 2 according to the registration message sent from the mobile computer 2, a user authenticating function which inspects the adequacy of the user of the mobile computer 2 by using information based upon a user input received from the mobile computer 2 prior to the registration by the registering function and controls the registration of the information on the current position by the registering function according to the inspection result, and a transfer function which

transfers packets addressed to the mobile computer to the current position of the mobile computer 2 according to the information registered by the registering function.

(C)1999,JPO

(19)日本国特許庁（ＪＰ）　(12)公開特許公報(A)　(11)特許出願公開番号

特開平11－161618

(43)公開日　平成11年(1999)６月18日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/16	６２０	Ｇ０６Ｆ	15/16	６２０Ｗ
	13/00	３５１		13/00	３５１Ｚ
	15/00	３３０		15/00	３３０Ａ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｃ
	12/46			11/00	３１０Ｃ

審査請求　未請求　請求項の数14　ＯＬ　(全 14 頁)　最終頁に続く

(21)出願番号　特願平10－249863

(22)出願日　平成10年(1998)９月３日

(31)優先権主張番号　特願平9－241163

(32)優先日　平９(1997)９月５日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　井上　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　石山　政浩
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　福本　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(74)代理人　弁理士　鈴江　武彦　(外６名)

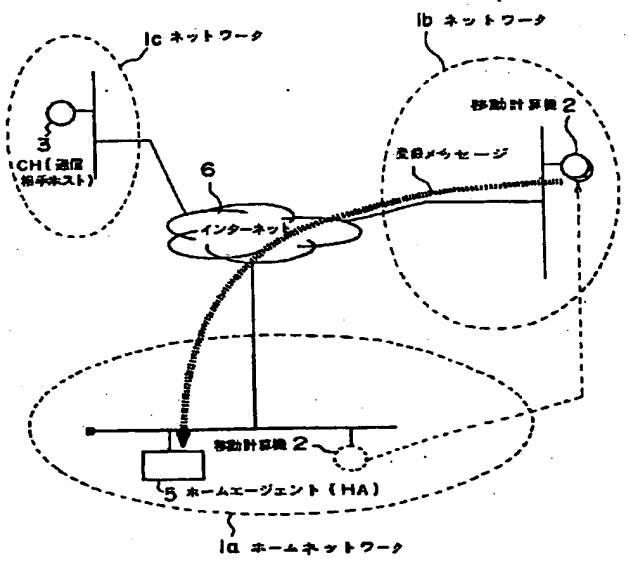
最終頁に続く

(54)【発明の名称】　移動計算機管理装置、移動計算機装置及び移動計算機登録方法

(57)【要約】

【課題】　移動計算機が移動先ネットワークから現在位置の登録メッセージを移動計算機管理装置（ホームエージェント）に送信する際に、移動計算機を操作しているユーザを認証することのできる移動計算機管理装置を提供すること。

【解決手段】　移動計算機のホームネットに設置され移動計算機がネットワーク間を移動して通信を行えるようにする移動計算機管理装置にて、該移動計算機から送信された登録メッセージに基づき該移動計算機の現在位置の情報を登録するための登録機能と、該登録機能による登録の実行に先立ち該移動計算機から受信したユーザ入力に基づく情報を用いて該移動計算機のユーザの正当性を検査しこの検査結果に基づいて該登録機能による該現在位置の情報の登録の実行を制御するユーザ認証機能と、該登録機能により登録が実行された情報に基づき移動計算機宛のパケットを該移動計算機の現在位置に転送する転送機能とを有する。



1

【特許請求の範囲】

【請求項１】移動計算機のホームネットワークに設置され、該移動計算機がネットワーク間を移動して通信を行えるようにする移動計算機管理装置であって、

前記移動計算機から送信された登録メッセージに基づき、該移動計算機の現在位置の情報を登録するための登録手段と、

前記登録手段による登録の実行に先立ち、前記移動計算機から受信したユーザ入力に基づく情報を用いて、該移動計算機のユーザの正当性を検査し、この検査結果に基づいて、前記登録手段による前記現在位置の情報の登録の実行を制御するユーザ認証手段と、

前記登録手段により登録が実行された情報に基づき、移動計算機宛のパケットを該移動計算機の現在位置に転送する転送手段とを備えたことを特徴とする移動計算機管理装置。

【請求項２】前記登録手段による登録の実行に先立ち、前記移動計算機から受信した登録メッセージに基づいて、該移動計算機の正当性を検査し、該移動計算機と該移動計算機のユーザの双方の正当性が確認された場合に、前記登録手段による前記現在位置の情報の登録の実行を許可するように制御するホスト認証手段を更に備えることを特徴とする請求項１に記載の移動計算機管理装置。

【請求項３】新規の登録メッセージを前記移動計算機から受信した場合に、前記登録手段による登録の実行に先立ち、該移動計算機に対してユーザ認証のための情報の返送を要求する返送要求メッセージを送信する送信手段を更に備え、

前記ユーザ認証手段は、この返送要求メッセージに応えて前記移動計算機から返送されてきた、前記ユーザ認証のための情報として該移動計算機へのユーザ入力に基づく情報が書き込まれた応答メッセージ中の、該ユーザに基づく情報を用いて、前記ユーザの正当性を検査するものであることを特徴とする請求項１に記載の移動計算機管理装置。

【請求項４】前記送信手段は、前記移動計算機から同じ現在位置について再登録を行うための登録メッセージを受信した場合、予め規定された条件により再度ユーザ認証を実行すべきことが示されていれば、前記登録手段により再登録を実行する前に、該移動計算機に対して前記返送要求メッセージを再度送信するものであることを特徴とする請求項３に記載の移動計算機管理装置。

【請求項５】前記再登録を行うための登録メッセージは、所定の間隔で受信され、前記送信手段に予め規定された条件は、前記返送要求メッセージを該所定の間隔よりも長い間隔をおいて送信するように定められていることを特徴とする請求項４に記載の移動計算機管理装置。

【請求項６】同一の前記移動計算機について、返送された前記応答メッセージからは前記ユーザの正当性が確認

2

されなかったことが、予め規定された回数連続した場合には、これ以降は該移動計算機からの登録要求を拒否することを特徴とする請求項４または５に記載の移動計算機管理装置。

【請求項７】前記ユーザ認証を要求するメッセージにはチャレンジコードを含め、

前記移動計算機から前記ユーザ入力に基づく情報として返された前記チャレンジコードに基づくワンタイムパスワードを検査することによりユーザの正当性を判断することを特徴とする請求項３ないし５のいずれか１項に記載の移動計算機管理装置。

【請求項８】前記移動計算機から前記ユーザ入力に基づく情報として返されたパスワードが予め登録されたものと一致するか否かによりユーザの正当性を判断することを特徴とする請求項１ないし５のいずれか１項に記載の移動計算機管理装置。

【請求項９】相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、

自装置のホームネットワークの外部の移動先から、該ホームネットワークに設置された、自装置宛のパケットを自装置の現在位置へ転送する手段を有する移動計算機管理装置宛に、現在位置の情報を含む登録メッセージを送信する送信手段と、

ユーザ認証のためのユーザ入力を受け付ける受付手段と、

前記登録メッセージを受信した前記移動計算機管理装置から返信された、ユーザ認証のための情報の返送を要求する返送要求メッセージを受信した場合、前記ユーザ入力に基づく情報を前記ユーザ認証のための情報として書き込んだ応答メッセージを前記移動計算機管理装置宛に返送する返送手段とを備えたことを特徴とする移動計算機装置。

【請求項１０】前記移動計算機管理装置から受信した前記返送要求メッセージに基づいて、該移動計算機管理装置の正当性を判断する手段を更に備え、

前記返送手段は、前記移動計算機管理装置が正当なものであると判断された場合に、前記ユーザ入力に基づく情報を含む前記応答メッセージを返送するものであることを特徴とする請求項９に記載の移動計算機装置。

【請求項１１】返送した前記応答メッセージに対して前記移動計算機管理装置からユーザの正当性が確認されなかった旨を示すメッセージが送信されてきたことが、予め規定された回数連続した場合には、これ以降の自装置からの登録要求メッセージの送出を抑止することを特徴とする請求項９または１０に記載の移動計算機装置。

【請求項１２】移動計算機を、該移動計算機がネットワーク間を移動して通信を行えるように、移動計算機の現在位置情報を管理し該移動計算機宛のパケットを該移動計算機の現在位置へ転送する移動計算機管理装置に対して、登録する方法であって、

前記移動計算機は、自装置のホームネットワークの外部の移動先に接続された場合、該ホームネットワークに設置された前記移動計算機管理装置宛に、現在位置の情報を含む登録メッセージを送信し、

前記移動計算機管理装置は、前記移動計算機から送信されたユーザ入力に基づく情報を用いて、該移動計算機のユーザの正当性を検査し、該ユーザが正当であると判断された場合に、該移動計算機の現在位置の登録を行うことを特徴とする移動計算機登録方法。

【請求項13】移動計算機のホームネットワークに設置され、該移動計算機がネットワーク間を移動して通信を行えるようにする移動計算機管理装置における移動計算機登録方法であって、

前記移動計算機から送信された登録メッセージに基づき該移動計算機の現在位置の情報を登録する際に、この登録の実行に先立ち、該移動計算機から受信したユーザ入力に基づく情報を用いて該移動計算機のユーザの正当性を検査し、この検査結果に基づいて該現在位置の情報の登録の実行を制御し、

前記登録が実行された情報に基づき、移動計算機宛のパケットを該移動計算機の現在位置に転送することを特徴とする移動計算機登録方法。

【請求項14】相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置における移動計算機登録方法であって、

自装置のホームネットワークの外部の移動先から、該ホームネットワークに設置された、自装置宛のパケットを自装置の現在位置へ転送する手段を有する移動計算機管理装置宛に、現在位置の情報を含む登録メッセージを送信し、

前記登録メッセージを受信した前記移動計算機管理装置から返信された、ユーザ認証のための情報の返送を要求する返送要求メッセージを受信した場合、ユーザ入力に基づく情報を前記ユーザ認証のための情報として書き込んだ応答メッセージを前記移動計算機管理装置宛に返送することを特徴とする移動計算機登録方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、相互接続している複数のネットワーク間で相互にデータを交換し必要なサービスを提供する複数の計算機により構成されるシステムにおける、ネットワーク間を移動して通信を行うことが可能な移動計算機装置、移動計算機の移動位置情報を管理し移動計算機宛のパケットを移動計算機の現在位置に転送する移動計算機管理装置及び移動計算機登録方法に関する。

【0002】

【従来の技術】計算機システムの小型化、低価格化やネットワーク環境の充実に伴って、計算機システムの利用は急速にかつ種々の分野に広く拡大し、また集中型システムから分散型システムへの移行が進んでいる。特に近年では計算機システム自体の進歩、能力向上に加え、コンピュータ・ネットワーク技術の発達・普及により、オフィス内のファイルやプリンタなどの資源共有のみならず、オフィス外、一組織外とのコミュニケーション（電子メール、電子ニュース、ファイルの転送など）が可能になり、これらが広く利用されはじめた。特に近年では、世界最大のコンピュータネットワーク「インターネット（internet）」の利用が普及しており、インターネットと接続し、公開された情報、サービスを利用したり、逆にインターネットを通してアクセスしてくる外部ユーザに対し、情報、サービスを提供することで、新たなコンピュータビジネスが開拓されている。また、インターネット利用に関して、新たな技術開発、展開がなされている。

【0003】また、このようなネットワークの普及に伴い、移動通信（mobile computing）に対する技術開発も行われている。移動通信では、携帯型の端末、計算機を持ったユーザがネットワーク上を移動して通信する。ときには通信を行いながらネットワーク上の位置を変えていく場合もあり、そのような通信において変化する移動計算機のネットワーク上のアドレスを管理し、正しく通信内容を到達させるための方式が必要である。

【0004】一般に移動通信を行う場合、移動計算機が所属していたネットワークに移動計算機の移動先データを管理するルータ（ホームエージェント）を置き、移動計算機が移動した場合、このホームエージェントに対して現在位置を示す登録メッセージを送る。登録メッセージが受け取られたら、移動計算機宛データの送信はそのホームエージェントを経由して、移動計算機の元のアドレス宛のIPパケットを移動計算機の現在位置アドレス宛パケット内にカプセル化することで移動計算機に対するデータの経路制御が行われる。例えば、図1では、元々ホームネットワーク1aに属していた移動計算機2が、他のネットワーク1bに移動し、ネットワーク1c内の他の計算機（CH）3との間で通信を行う場合に、移動計算機2に対しホームエージェント（HA）5が上記の役割を行う。この方式は、インターネットの標準化団体であるIETFのmobile-IPワーキンググループで標準化が進められている移動IPと呼ばれる方式である（文献：RFC2002, IP mobility support (C. Perkins)）。

【0005】ところで、移動IP方式では、移動計算機が新規の移動先に移った場合、現在位置の登録メッセージをホームエージェントに送ることが必要である。移動計算機への成り済ましなどの攻撃を回避するため、位置登録メッセージには移動計算機とホームエージェント間で予め交換したセキュリティ情報に従って認証コードが付加される。正しい認証コードが付加された登録メッセ

5

ージでないと、移動計算機の位置登録は行われない。

【０００６】しかしながら、移動ＩＰで規定されているセキュリティ対策はあくまでホスト（移動計算機）単位のセキュリティであり、その移動計算機を使用しているユーザの実体を認証するものではない。すなわち、例えば移動計算機にホスト間の認証のためのセキュリティ情報が保持されたまま、不正なユーザにホスト自体が盗まれると、不正なユーザが正規ユーザに成り済まして、ホームネットワーク上の情報を取り出すことができ非常に危険である。

【０００７】また、ホストを盗まれなくても、正規ユーザが登録処理までを行った移動計算機を一時的に借用するだけで、ホームネットワーク上の機密情報を取り出されてしまうことも考えられる。

【０００８】すなわち、従来の移動ＩＰ方式におけるセキュリティ対策では、ホスト単位の成り済ましには対応されているが、不正ユーザが正規ユーザに成り済ますという攻撃には極めて弱いといえる。そのため、移動先（外部ネットワーク）に内部ネットワークの機密情報が取り出されてしまうおそれがあった。

【０００９】

【発明が解決しようとする課題】従来の移動ＩＰ方式におけるセキュリティ対策では、ホスト単位の成り済ましには対応されているが、不正ユーザが正規ユーザに成り済ますという攻撃には極めて弱いといえる。そのため、移動先（外部ネットワーク）に内部ネットワークの機密情報が取り出されてしまうおそれがあった。

【００１０】本発明は、上記事情を考慮してなされたもので、移動計算機が移動先ネットワークに接続し、現在位置の登録メッセージをホームエージェントに送信する際に、移動計算機を操作しているユーザを認証することのできる移動計算機管理装置、移動計算機装置及び移動計算機登録方法を提供することを目的とする。

【００１１】また、本発明は、一旦移動計算機が現在位置の登録メッセージをホームエージェントに送信した後も、定期的にユーザ認証を行い、セッション確立後に不正ユーザが移動計算機を使用するケースにも対応できる移動計算機管理装置、移動計算機装置及び移動計算機登録方法を提供することを目的とする。

【００１２】

【課題を解決するための手段】本発明（請求項１）は、移動計算機のホームネットワークに設置され、該移動計算機がネットワーク間を移動して通信を行えるようにする移動計算機管理装置（ホームエージェント）であって、前記移動計算機から送信された登録メッセージに基づき、該移動計算機の現在位置の情報を登録するための登録手段と、前記登録手段による登録の実行に先立ち、前記移動計算機から受信したユーザ入力に基づく情報を用いて、該移動計算機のユーザの正当性を検査し、この検査結果に基づいて、前記登録手段による前記現在位置

6

の情報の登録の実行を制御するユーザ認証手段と、前記登録手段により登録が実行された情報に基づき、移動計算機宛のパケットを該移動計算機の現在位置に転送する転送手段とを備えたことを特徴とする。

【００１３】好ましくは、前記登録手段による登録の実行に先立ち、前記移動計算機から受信した登録メッセージに基づいて、該移動計算機の正当性を検査し、該移動計算機と該移動計算機のユーザの双方の正当性が確認された場合に、前記登録手段による前記現在位置の情報の登録の実行を許可するように制御するホスト認証手段を更に備えるようにしてもよい。

【００１４】好ましくは、新規の登録メッセージを前記移動計算機から受信した場合に、前記登録手段による登録の実行に先立ち、該移動計算機に対してユーザ認証のための情報の返送を要求する返送要求メッセージを送信する送信手段を更に備え、前記ユーザ認証手段は、この返送要求メッセージに応えて前記移動計算機から返送されてきた、前記ユーザ認証のための情報として該移動計算機へのユーザ入力に基づく情報が書き込まれた応答メッセージ中の、該ユーザに基づく情報を用いて、前記ユーザの正当性を検査するものであるようにしてもよい。

【００１５】好ましくは、前記送信手段は、前記移動計算機から同じ現在位置について再登録を行うための登録メッセージを受信した場合、予め規定された条件により再度ユーザ認証を実行すべきことが示されていれば、前記登録手段により再登録を実行する前に、該移動計算機に対して前記返送要求メッセージを再度送信するものであるようにしてもよい。

【００１６】好ましくは、前記再登録を行うための登録メッセージは、所定の間隔で受信され、前記送信手段に予め規定された条件は、前記返送要求メッセージを該所定の間隔よりも長い間隔をおいて送信するように定められているようにしてもよい。

【００１７】また、予め規定された条件としては、例えば、前回にユーザ認証を行ってから予め規定された時間が経過していること、あるいは前回にユーザ認証を行うこととなった再登録を行うための登録メッセージの受信から今回の受信が予め規定された回数に当たること、などとしてもよい。なお、再登録を行うための登録メッセージを受信する毎に毎回、ユーザ認証を行うようにしても構わない。

【００１８】好ましくは、同一の前記移動計算機について、返送された前記応答メッセージからは前記ユーザの正当性が確認されなかったことが、予め規定された回数連続した場合には、これ以降は該移動計算機からの登録要求を拒否するようにしてもよい。

【００１９】好ましくは、前記ユーザ認証を要求するメッセージにはチャレンジコードを含め、前記移動計算機から前記ユーザ入力に基づく情報として返された前記チャレンジコードに基づくワンタイムパスワードを検査す

ることによりユーザの正当性を判断するようにしてもよい。

【0020】好ましくは、前記移動計算機から前記ユーザ入力に基づく情報として返されたパスワードが予め登録されたものと一致するか否かによりユーザの正当性を判断するようにしてもよい。

【0021】本発明（請求項9）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、自装置のホームネットワークの外部の移動先から、該ホームネットワークに設置された、自装置宛のパケットを自装置の現在位置へ転送する手段を有する移動計算機管理装置（ホームエージェント）宛に、現在位置の情報を含む登録メッセージを送信する送信手段と、ユーザ認証のためのユーザ入力を受け付ける受付手段と、前記登録メッセージを受信した前記移動計算機管理装置から返信された、ユーザ認証のための情報の返送を要求する返送要求メッセージを受信した場合、前記ユーザ入力に基づく情報を前記ユーザ認証のための情報として書き込んだ応答メッセージを前記移動計算機管理装置宛に返送する返送手段とを備えたことを特徴とする。

【0022】好ましくは、前記移動計算機管理装置から受信した前記返送要求メッセージに基づいて、該移動計算機管理装置の正当性を判断する手段を更に備え、前記返送手段は、前記移動計算機管理装置が正当なものであると判断された場合に、前記ユーザ入力に基づく情報を含む前記応答メッセージを返送するものであるようにしてもよい。

【0023】好ましくは、返送した前記応答メッセージに対して前記移動計算機管理装置からユーザの正当性が確認されなかった旨を示すメッセージが送信されてきたことが、予め規定された回数連続した場合には、これ以降の自装置からの登録要求メッセージの送出を抑止するようにしてもよい。

【0024】本発明（請求項12）は、移動計算機を、該移動計算機がネットワーク間を移動して通信を行えるように、移動計算機の現在位置情報を管理し該移動計算機宛のパケットを該移動計算機の現在位置へ転送する移動計算機管理装置（ホームエージェント）に対して、登録する、移動計算機登録方法であって、前記移動計算機は、自装置のホームネットワークの外部の移動先に接続された場合、該ホームネットワークに設置された前記移動計算機管理装置宛に、現在位置の情報を含む登録メッセージを送信し、前記移動計算機管理装置は、前記移動計算機から送信されたユーザ入力に基づく情報を用いて、該移動計算機のユーザの正当性を検査し、該ユーザが正当であると判断された場合に、該移動計算機の現在位置の登録を行うことを特徴とする。

【0025】本発明（請求項13）は、移動計算機のホームネットワークに設置され、該移動計算機がネットワーク間を移動して通信を行えるようにする移動計算機管理装置（ホームエージェント）における移動計算機登録方法であって、前記移動計算機から送信された登録メッセージに基づき該移動計算機の現在位置の情報を登録する際に、この登録の実行に先立ち、該移動計算機から受信したユーザ入力に基づく情報を用いて該移動計算機のユーザの正当性を検査し、この検査結果に基づいて該現在位置の情報の登録の実行を制御し、前記登録が実行された情報に基づき、移動計算機宛のパケットを該移動計算機の現在位置に転送することを特徴とする。

【0026】本発明（請求項14）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置における移動計算機登録方法であって、自装置のホームネットワークの外部の移動先から、該ホームネットワークに設置された、自装置宛のパケットを自装置の現在位置へ転送する手段を有する移動計算機管理装置（ホームエージェント）宛に、現在位置の情報を含む登録メッセージを送信し、前記登録メッセージを受信した前記移動計算機管理装置から返信された、ユーザ認証のための情報の返送を要求する返送要求メッセージを受信した場合、ユーザ入力に基づく情報を前記ユーザ認証のための情報として書き込んだ応答メッセージを前記移動計算機管理装置宛に返送することを特徴とする。

【0027】なお、以上の装置に係る発明は方法に係る発明としても成立し、方法に係る発明は装置に係る発明としても成立する。また、上記の発明は、相当する手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体としても成立する。

【0028】従来の移動ＩＰ方式におけるセキュリティ対策では、ホスト単位の成り済ましには対応されているが、不正ユーザが正規ユーザに成り済ますという攻撃には極めて弱い、といえる。そのため、移動先（外部ネットワーク）に内部ネットワークの機密情報が取り出されてしまうおそれがあった。

【0029】本発明によれば、移動計算機が移動先ネットワークに接続し、現在位置の登録メッセージを移動計算機管理装置（ホームエージェント）に送信する際に、移動計算機と移動計算機管理装置との間で、登録された正当なユーザでなければ知得できない情報をやり取りするので、移動計算機を操作しているユーザを認証することができ、より安全に移動計算機を運用することができる。

【0030】また、本発明によれば、一旦移動計算機が現在位置登録メッセージを移動計算機管理装置（ホームエージェント）に送信した後も、定期的にユーザ認証を行い、セッション確立後に不正ユーザが移動計算機を使用するケースにも対応できる。また、不正ユーザが一定回数以上認証に失敗した場合に、それ以降の登録を不可とすることができる。この結果、移動計算機の盗難やユ

ーザ詐称による不正動作を防止できる。

【0031】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。図1に、本実施形態に係る通信システムの基本構成の一例を示す。図1の通信システムは、移動IP（RFC2002）により移動計算機の通信をサポートしているものとする。なお、移動IPプロトコルでは、移動先ネットワークで移動計算機に対するパケット配送を行うフォーリンエージェントというルータの存在を仮定するモードと、フォーリンエージェントを設けない（移動計算機自身がフォーリンエージェントを兼ねる）Co－located Care－of addressモードがあるが、本実施形態では、後者を採用するものとして説明する。

【0032】図1では、ホームネットワーク1a、第1の他部署ネットワーク1b、第2の他部署ネットワーク1cがインターネット6を介して相互に接続されており、移動計算機（MN）2、移動計算機の通信相手（CH）3は、これらネットワーク内に接続され、または外部ノードとしてインターネット6に接続される。

【0033】本実施形態では、ネットワーク1aの内部をホームポジションとする移動計算機2が他部署ネットワーク1bに移動した場合について説明する。ホームネットワーク1aには、移動IPプロトコルをサポートするために、移動計算機の移動先の現在位置の情報を管理するホームエージェント（HA）5が設けられる。管理対象とする移動計算機の台数は任意である。前述したように、移動中の移動計算機2宛に転送されてきたIPパケットは、そのホームエージェント5を経由し、移動計算機2の元のアドレス（ホームネットワーク1aにおけるアドレス）宛のIPパケットを移動IP形式の現在位置アドレス宛てパケット内にカプセル化することで、移動計算機2に対するデータの経路制御を行うことができる。

【0034】移動計算機2は、自装置がホームネットワーク外に移動した場合には、移動先のネットワーク（ここでは1b）において、例えばDHCPやPPPなどのプロトコルにより移動先ネットワークで使用するアドレスを獲得する。アドレスを獲得したら、移動計算機2は、ホームネットワーク1aのホームエージェント5に現在位置の情報を含む登録メッセージを送信する。

【0035】図2に移動計算機2からホームエージェント5に送信される登録メッセージの形式を示す。フラグ（FLAG）は移動IPの動作モード（カプセル化の方法など）を示す。

【0036】Lifetimeはこの登録の有効期限を示す。移動計算機2は有効期限を越えた場合、再度登録メッセージをホームエージェント5に送信し、再登録を行わなくてはいけない。

【0037】Home Addressは移動計算機の

ホーム位置を、Care－of Addressは移動計算機の現在位置を、Home Agentはホームエージェント5のアドレスを示す。

【0038】Identificationは登録に対するIDでリプレイ攻撃を防止するために付加される。Extensionsには少なくとも移動計算機2～ホームエージェント5間の（ホスト認証のための）認証情報が含まれる。このExtension部分を図3に示す。SPIは両者の間で交換したセキュリティパラメータインデックスを、Authenticatorは認証コードを示す。

【0039】この登録メッセージをホームエージェント5が受信し、正しく登録処理が行われた場合、図4に示す登録応答メッセージが移動計算機2に返される。codeには登録成功を示す応答コード0または1が記述される。一方、登録に失敗した場合、図4と同じ形式の登録応答メッセージが移動計算機2に返される。この場合には、種々の登録失敗の理由を示す応答コードが記述される。

【0040】以下に、応答コード（Reply codes）の一覧を示す。左側の数字がコードであり、右側の説明がそのコードの示す意味内容である。

＜成功（success）のケース＞

0：登録受諾（registration accepted）

1：登録受諾だが、同時移動バインドはサポートしない（registration accepted, but simultaneous mobility bindings unsupported）

＜フォーリンエージェントのための失敗（failure for Foreign agent）のケース＞

64：理由不明（reason unspecified）

65：管理上の理由で禁止（administratively prohibited）

66：リソースが不十分（insufficient resources）

67：移動ノードの認証失敗（mobile node failed authentication）

68：ホームエージェントが認証に失敗（home agent failed authentidation）

69：要求されたLifeitmeが長すぎる（requested Lifetime too long）

70：要求の形式が正しくない（poorly formed Request）

71：応答の形式が正しくない（poorly formed Reply）

72：要求のカプセル化が使用できない（requested encapsulation unavail

able）
73：要求のVan Jacobson圧縮が使用できない（requested Van Jacobson compression unavailable）
80：ホームネットワークが到達不能（ICMPエラー受信）（home network unreachable（ICMP error received））
81：ホームエージェント・ホストが到達不能（ICMPエラー受信）（home agent host unreachable（ICMP errorreceived））
82：ホームエージェント・ポートが到達不能（ICMPエラー受信）（home agent port unreachable（ICMP errorreceived））
88：ホームエージェントが到達不能（ICMPエラー受信）（home agent unreachable（ICMP error received））
<ホームエージェントのための失敗（failure for Home agent）のケース>
128：理由不明（reason unspecified）
129：管理上の理由で禁止（administratively prohibited）
130：リソースが不十分（insufficient resources）
131：移動ノードの認証失敗（mobile node failed authentication）
132：フォーリンエージェントが認証に失敗（foreign agentfailed authentecation）
133：登録識別子がマッチしない（registration Identfication mismatch）
134：要求の形式が正しくない（poorly formed Request）
135：同時移動バインド数が多すぎる（too many simultaneous mobility bindings）
136：未知のホームエージェント・アドレス（unknown homeagent address）
さて、本実施形態では、ホームエージェント5が移動計算機2から登録メッセージを受信しても、すぐには登録処理を行わず、該移動計算機2のユーザ認証を行い、ユーザ認証に成功した場合にのみ登録処理を行う。

【0041】以下では、ホームエージェント5が移動計算機2を使用しているユーザを認証するため、チャレンジ～レスポンスによるメッセージを交換する例を、図5を参照しながら説明する。

【0042】チャレンジメッセージの形式を図6（a）

に、レスポンスメッセージの形式を図6（b）に示す。この例では、移動計算機2が登録要求メッセージをホームエージェント5に送信すると、ホームエージェント5は、まず、認証情報を調べホスト認証を行う。そして、ホスト認証に成功したならば、ホームエージェント5は、パスワード入力を要求するチャレンジメッセージを、移動計算機2に返信する。

【0043】移動計算機2は、このチャレンジメッセージを受けると、メッセージを表示するなどして、ユーザにパスワード入力を促す。そして、パスワードが入力されたならば、このユーザが入力したパスワードを書き込んだレスポンスメッセージを、ホームエージェント5に送信する。

【0044】レスポンスメッセージを受け取ったホームエージェント5は、予めホームネットワーク駐在時に該移動計算機に対応して登録してあったパスワードと比較を行い、照合の結果、該移動計算機から返されたパスワードが正しいものであることが確認されたならば、現在位置の登録を許可するものとし、登録成功の応答コードを含む登録応答メッセージを返信するとともに、現在位置を登録して移動計算機2へのデータパケットの転送を開始する。

【0045】このようにホームエージェント5側でパスワード認証を行うことで、移動計算機内にユーザ認証のための情報を搭載して携帯することが不要になり、移動計算機の盗難などの危険を回避することができる。また、システム全体の管理者が移動中の計算機の利用パスワードについても、ホームエージェント5上で一元管理できるので、計算機の不正使用など異常な状態になった場合も対応が容易であり、より安全なシステム運用を可能とすることができる。

【0046】さらに、ホームエージェント側では、移動IPの登録メッセージを送信してきたホストが正当なホストであるかどうかの検証と、移動IP通信しようとしているユーザが正当なユーザであるかどうかの検証とを独立に運用することができるので、ユーザとホスト（移動計算機）との任意の組合せに対して移動IP通信を許可することも可能である。すなわち、例えばホームエージェントではなくホストとユーザとの間でユーザ認証を行い、ホストとホームエージェントとの間でホスト認証を行うようなシステムでは、ホストとユーザの組合せが固定でなければ認証できないのに対して、より柔軟な管理も可能になる。

【0047】なお、以降の再登録メッセージについては、同様の手順でその都度ユーザ認証を行う方法、何回かに一度だけユーザ認証を行う方法、ユーザ認証を行わない方法など種々の方法が考えられる。

【0048】また、上記では、移動計算機からホームエージェント5にパスワードを返したが、パスワードとユーザIDの組を返し、ホームエージェント5はこの組が

予め登録されたものかどうか調べることによりユーザの正当性を判断するようにしてもよい。

【0049】なお、上記では移動計算機からホームエージェントへの登録要求に対してまずホスト認証を行い、パスワード送信を促すメッセージがホームエージェントから移動計算機へ返ってきてから改めてユーザ認証の手続きを行う例を説明したが、最初の登録要求を移動計算機が送信する際にパスワードも含めて送信することにより、ホスト認証とユーザ認証をワンステップで行ってしまうことも可能である。

【0050】ただし、登録要求によるホスト認証とパスワード送信によるユーザ認証のステップを分離したり、あるいはユーザ認証の際にユーザ名とパスワードを2度に分けて送ることで、より強固なセキュリティに基づいた管理を行うことも可能である。後者の場合、例えば、ユーザ名を最初に送り、これを受けたホームエージェント5は予め各ユーザに対し登録された初期データを元にワンタイムパスワードのチャレンジメッセージを返す。これに対して改めてユーザがレスポンスメッセージを返すことで正規の登録が行われる、という方式をとる。また、前者の場合、登録要求に対するホームエージェントからの返信メッセージを受信した移動計算機が、通信相手が正当なホームエージェントであるかどうかを検証した後でユーザ認証の情報（パスワード）を送ることができる。

【0051】このように登録要求とユーザ認証情報を1セットとして処理を行うか、ユーザ名とパスワードを1セットとして処理を行うか、これらを別のメッセージとして扱うかに関しては、システムのセキュリティに対する要求仕様、移動計算機側のユーザインタフェースに関する要求仕様に応じて決定すべきである。

【0052】上記の例では、単純なパスワード照合によるユーザ認証の例を示したが、ユーザ認証には他の方法を使用することもできる。例えばワンタイムパスワードにより認証を行う方法が考えられる。以下ではワンタイムパスワードを用いたユーザ認証の例を図7を参照しながら説明する。

【0053】チャレンジメッセージの形式を図8（a）に、レスポンスメッセージの形式を図8（b）に示す。この例では、移動計算機2が登録要求メッセージをホームエージェント5に送信すると、まず、ホームエージェント5は認証情報を調べホスト認証を行っう。そして、ホスト認証に成功したならば、この移動計算機2を使用するユーザの登録情報をもとにしてワンタイムパスワードのチャレンジコードを求める。そして、このチャレンジコードを付加した、パスワード入力を要求するチャレンジメッセージを、移動計算機2に返信する。

【0054】チャレンジメッセージを受信した移動計算機2は、別のユーティリティを使用して、このチャレンジメッセージ内のワンタイムパスワードチャレンジコードとユーザから入力されたパスワードとが反映された、このチャレンジに対して応答するデータを算出し、このデータを含むレスポンスメッセージをホームエージェント5に送信する。

【0055】レスポンスメッセージを受け取ったホームエージェント5は、登録情報をもとに移動計算機2で行われたものと同じ計算を行って、データの照合を行い、正しければ、現在位置の登録を許可するものとし、登録成功の応答コードを含む登録応答メッセージを返信するとともに、現在位置を登録して移動計算機2へのデータパケットの転送を開始する。

【0056】なお、以降の再登録メッセージについては、同様の手順でその都度ユーザ認証を行う方法、何回かに一度だけユーザ認証を行う方法、ユーザ認証を行わない方法など種々の方法が考えられる。

【0057】なお、上記の各例においてユーザ認証が失敗に終わった場合、ただちにユーザ認証不成功を示すコードを含む登録応答メッセージを該移動計算機に返すようにしてもよい。あるいは、チャレンジメッセージとレスポンスメッセージのやり取りを規定回数繰り返してもユーザ認証に成功しなかった場合に、ユーザ認証不成功を示すコードを含む登録応答メッセージを該移動計算機に返すようにしてもよい。

【0058】上記の2つの例では、移動計算機2が移動先ネットワークに接続し、登録処理を開始する時点でのユーザ認証について示したが、実際の運用では登録完了後に不正ユーザが移動計算機2を不正使用して（例えば、正規ユーザが移動計算機2を繋いだまま離席し、その間に不正ユーザが使用するなど）、ホームネットワーク内の情報を漏洩させるようなケースにも対応することが望ましい。

【0059】このための対応処理として、移動計算機2が一旦登録処理に成功した後も、一定時間毎にホームエージェント5から移動計算機2にユーザ認証要求メッセージを送信することが考えられる。そのような例を図9および図10を参照しながら説明する。図9はこの場合にホームエージェント5に付加する機能を示すブロック図の一例であり、図10はその手順の一例である。

【0060】図9の機能を持つホームエージェント5において、予めユーザ（またはシステム管理者）が指定する再ユーザ認証インターバル時間をレジスタ51に入力する。

【0061】ある移動計算機2について、ユーザ認証シーケンスを実行すると（ステップS15）、その移動計算機2に対応するタイマカウンタ52は0にクリアされる（ステップS11）。なお、最初のユーザ認証シーケンスは、例えば図5や図7のように、ある移動計算機について、移動後の最初の登録メッセージを受信したときである。

【0062】その後、移動計算機から現在位置の再登録

メッセージを受信し、再登録を行う毎に、該当するタイマカウンタ５２が経過時間に更新される（ステップＳ１２～Ｓ１４）。

【００６３】この位置再登録時には、レジスタ５１のインターバル時間と該当するタイマカウンタ５２の値が比較部５３にて比較され（ステップＳ１４）、タイマカウンタ５２の内容がインターバル時間より小さい場合は、ユーザ認証なしに現在位置の再登録および登録成功メッセージの送信を行う。

【００６４】一方、タイマカウンタ５２の内容がインターバル時間に達した場合には、例えば図５や図７のようなユーザ認証シーケンスを、再度実行する（ステップＳ１５）。ユーザ認証が正しく行われると、現在位置の再登録を許可するものとし、登録成功の応答コードを含む登録応答メッセージを返信するとともに、現在位置の再登録を行って移動計算機２へのデータパケットの転送を継続し、また、再度、該当するタイマカウンタ５２は０にクリアされる（ステップＳ１１）。

【００６５】そして、ユーザ認証なしの位置再登録およびタイマーカウンタの更新の繰り返えしと、一定時間経過した場合のユーザ認証とこれに成功した際の位置再登録といった、一連の手順が、現在位置の有効期限の経過またはユーザ認証の失敗または位置登録の失敗まで繰り返される。

【００６６】また、ユーザ認証が失敗に終わった場合、前述したように、ただちにユーザ認証不成功を示すコードを含む登録応答メッセージを該移動計算機に返すようにしてもよいし、チャレンジメッセージとレスポンスメッセージのやり取りを規定回数繰り返してもユーザ認証に成功しなかった場合に、ユーザ認証不成功を示すコードを含む登録応答メッセージを該移動計算機に返すようにしてもよい。

【００６７】なお、上記では、一定時間経過ごとにユーザ認証を行う例を示したが、再登録メッセージを受信するごとにユーザ認証を行う方法、何回かに一度だけユーザ認証を行う方法など、種々の方法が考えられる。

【００６８】ところで、例えば移動計算機２が盗難されて、不正ユーザがホームネット外部から登録要求を行おうとする場合、図５、図７、図１０で例示したようなユーザ認証を用いれば、（通常の方法ではユーザ認証を成功させるのは極めて困難であるので）現在位置の登録ができず、不正使用はできない。しかし、不正ユーザがパスワードを総当たりで破ろうとするなどして、登録（ユーザ認証）メッセージの送受信を繰り返し行うことで、ホームネットワークのトラフィックが混雑し、正常な運用ができなくなるおそれがある。また、不正ユーザから辞書などを使ったパスワードの類推攻撃を受ける可能性も考えられる。

【００６９】これらの問題に対応するため、一定回数のユーザ認証失敗を繰り返した場合、以降の移動計算機２からのメッセージ送出を不可能とすることが考えられる。そのような例を図１１および図１２を参照しながら説明する。図１１はこの場合に移動計算機２に付加する機能を示すブロック図の一例であり、図１２はその手順の一例である。

【００７０】図１１の機能を持つ移動計算機２において、予めユーザ（システム管理者あるいは移動計算機の使用者等）が指定する連続ユーザ認証失敗回数をレジスタ１２１に入力する（ステップＳ２１）。

【００７１】移動計算機２がユーザ認証に失敗した旨のメッセージをホームエージェント５から受信する毎に、（予め初期化しておいた）失敗回数カウンタ１２２をインクリメントする（ステップＳ２２～Ｓ２５）。一方、ユーザ認証に成功したら（ステップＳ２３でＹｅｓの場合）、失敗回数カウンタ１２２は０にリセットされる。

【００７２】しかして、ステップＳ２５において、比較部１２３にてレジスタ１２１と認証失敗回数カウンタ１２２の値を比較して、それらが一致したら（ステップＳ２５でＹｅｓの場合）、移動計算機２はメッセージ送出停止制御部１２４を起動し、これ以降の一切のメッセージ送出を停止する（ステップＳ２６）。メッセージ送出停止制御部１２４によるメッセージ送信停止を解除するには、この移動計算機２に固有のホームエージェント内に格納されている情報を使用しなくてはいけないものとする。

【００７３】上記では移動計算機にメッセージ送信抑止機能を設けたが、他の例（図１３、図１４）として、ホームエージェント５側でユーザ認証失敗回数カウンタ１５２を持ち、失敗回数レジスタ１５１の値がこれに同じくなったら、それ以降いかなるメッセージが送信されても登録を成功させないという方法も考えられる。

【００７４】この場合、図１３の機能を持つホームエージェント５において、予めユーザ（システム管理者等）が指定する連続ユーザ認証失敗回数を、各移動移動計算機に対応するレジスタ１５１に入力する（ステップＳ３１）。

【００７５】ホームエージェント５では、ユーザ認証が成功しなかった毎に、該当する（予め初期化しておいた）失敗回数カウンタ１５２をインクリメントする（ステップＳ２３～Ｓ２５）。一方、ユーザ認証に成功したら（ステップＳ３３でＹｅｓの場合）、失敗回数カウンタ１５２は０にリセットされる。

【００７６】しかして、ステップＳ３５において、比較部１５３にてレジスタ１５１と認証失敗回数カウンタ１５２の値を比較して、それらが一致したら（ステップＳ３５でＹｅｓの場合）、ホームエージェント５は登録メッセージ受付拒否制御部１５４を起動し、これ以降の当該移動計算機２からの一切の登録メッセージの受付を拒否する（ステップＳ２６）。

【００７７】なお、この方法は、不要なメッセージのや

り取りを防止できない点で、図１１、図１２の例よりセキュリティ的な基準は多少甘いとも考えられるが、例えばサイトのポリシーなどに依って図１１と図１３のいずれの方法を使用するかを選択するなどすればよい。

【００７８】また、上記した２つの例の他に、規定回数の失敗は移動計算機２側で検出し、これを移動計算機２からホームエージェント５に通知し、ホームエージェント５はそれ以降の当該移動計算機２からの一切の登録メッセージの受付を拒否するようにする方法も考えられる。

【００７９】上記の３つの例において、規定回数の認証の失敗を検出した時点で当該移動計算機２の登録を削除してもよいし、有効期限までは転送をサポートするようにしてもよい。

【００８０】次に、本実施形態に係るホームエージェント５の構成について説明する。図１５にホームエージェント５の要部構成例のブロック図を示す。図１５に示されるように、このホームエージェント５は、移動登録に関する処理を行う移動登録処理部２０１、移動登録以外に関する処理を行う通信処理部２０３、ネットワークへのデータ入出力処理を行うデータ入出力部２０２を有する。

【００８１】また、移動登録処理部２０１は、例えばパスワードなど認証に必要なデータを登録するためのユーザ認証データベース２１１、移動計算機に送信するチャレンジメッセージを生成する処理を行うためのチャレンジ生成部２１２、移動登録メッセージからパスワードを抽出する処理を行うためのパスワード抽出部２１３、移動登録メッセージからユーザ情報を抽出する処理を行うためのユーザ情報抽出部２１４、登録応答メッセージを生成する処理を行うための登録応答生成部２１５を有する。

【００８２】例えば、図５で示した認証手順の例の場合、まず、移動計算機２から送信された登録要求メッセージは、ネットワークを介しデータ入力部２０２から移動登録処理部２０１に伝えられる。そして、移動登録処理部２０１のユーザ情報抽出部２１４にて、登録要求メッセージとユーザ認証データベース２１１の内容に基づいてホスト認証を行い、ホスト認証に成功したならばチャレンジ生成部２１２にて、パスワード入力を要求するチャレンジメッセージを生成し、これをデータ入出力部２０２を介して移動計算機２に返信する。

【００８３】ここで、前述のように、移動計算機２は、このチャレンジメッセージを受けると、メッセージを表示するなどして、ユーザにパスワード入力を促す。そして、パスワードが入力されたならば、このユーザが入力したパスワードを書き込んだレスポンスメッセージを、ホームエージェント５に送信する。

【００８４】移動計算機２から送信されたレスポンスメッセージは。ネットワークを介しデータ入力部２０２から移動登録処理部２０１に伝えられる。そして、移動登録処理部２０１のパスワード抽出部２１３にて、レスポンスメッセージとユーザ認証データベース２１１の内容に基づいてユーザ認証を行い、ユーザ認証に成功したならば登録応答生成部２１５にて、登録成功の応答コードを含む登録応答メッセージを生成し、これをデータ入出力部２０２を介して移動計算機２に返信する。また、これとともに、該移動計算機の現在位置を登録して、該移動計算機へのデータパケットの転送を開始する。

【００８５】これまで説明した他の認証手順もこの移動登録処理部２０１によって実行可能である。もちろん、このホームエージェント５は、その全体もしくは一部をプログラムによって実現可能である。

【００８６】さて、従来の移動ＩＰ方式におけるセキュリティ対策では、ホスト単位の成り済ましには対応されているが、不正ユーザが正規ユーザに成り済ますという攻撃には極めて弱い、といえる。そのため、移動先（外部ネットワーク）に内部ネットワークの機密情報が取り出されてしまうおそれがあった。

【００８７】本実施形態によれば、移動計算機が移動先ネットワークに接続し、現在位置の登録メッセージをホームエージェントに送信する際に、移動計算機とホームエージェントとの間で、登録された正当なユーザでなければ知得できない情報をやり取りするので、移動計算機を操作しているユーザを認証することができ、より安全に移動計算機を運用することができる。

【００８８】また、本実施形態によれば、一旦移動計算機が現在位置登録メッセージをホームエージェントに送信した後も、定期的にユーザ認証を行い、セッション確立後に不正ユーザが移動計算機を使用するケースにも対応できる。また、不正ユーザが一定回数認証に失敗した場合に、それ以降の登録メッセージ送出を停止あるいは登録メッセージの受け付けを不許可とすることができる。

【００８９】この結果、移動計算機の盗難やユーザ詐称による不正動作を防止できる。なお、本実施形態では、Ｃｏ－ｌｃａｔｅｄ　Ｃａｒｅ－ｏｆ　Ａｄｄｒｅｓｓモードによる通信システムについて説明したが、本発明は、フォーリンエージェントの存在を仮定した移動通信システムにも適用可能である。

【００９０】また、本発明は、ＲＦＣ２００２に示される移動ＩＰだけでなく、他の様々な移動通信プロトコルに対しても適用可能である。また、以上の各機能、例えば処理の部分の他、移動計算機がユーザ認証を行う再登録回数を指定する設定カウンタ、登録回数をカウントするカウンタなどはハードウェアとしてもソフトウェアとしても実現可能である。また、上記した各手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体として実施することもできる。本発明は、上述した実施の形態に限定されるもので

はなく、その技術的範囲において種々変形して実施することができる。

【００９１】

【発明の効果】本発明によれば、移動先ネットワークに接続した移動計算機から現在位置の登録メッセージが移動計算機管理装置に送信された際に、移動計算機と移動計算機管理装置との間で、登録された正当なユーザでなければ知得できない情報をやり取りするので、移動計算機を操作しているユーザを認証することができる。この結果、移動計算機の盗難やユーザ詐称による不正動作を防止することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るネットワークの基本構成を示す図

【図２】同実施形態に係る移動計算機の送信する登録要求メッセージ形式を示す図

【図３】同実施形態に係る移動計算機の送信するホスト認証のための拡張した登録要求メッセージを示す図

【図４】同実施形態に係るホームエージェントからの登録要求応答メッセージを示す図

【図５】同実施形態に係るユーザ認証方式を説明するための図

【図６】ユーザ認証のためのメッセージの形式の一例を示す図

【図７】同実施形態に係る他のユーザ認証方式を説明するための図

【図８】ユーザ認証のためのメッセージの形式の他の例を示す図

【図９】位置再登録に伴うユーザ認証を行うホームルータの構成を示す図

【図１０】図９のホームルータの動作手順を示すフローチャート

【図１１】ユーザ認証に関する攻撃に対処する移動計算機の構成を示す図

*【図１２】図１１の移動計算機の動作手順を示すフローチャート

【図１３】ユーザ認証に関する攻撃に対処するホームルータの構成を示す図

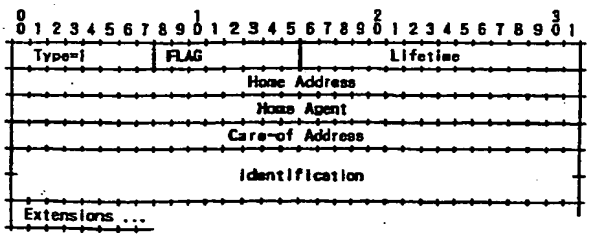
【図１４】図１１のホームエージェントの動作手順を示すフローチャート

【図１５】同実施形態に係るホームエージェントの構成例を示す図

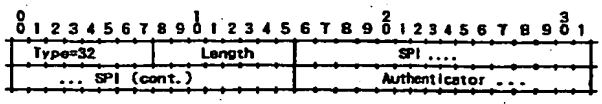
【符号の説明】

１ａ，１ｂ，１ｃ…ネットワーク
２…移動計算機
３…通信相手計算機
５…ホームエージェント
６…インターネット
５１…インターバルレジスタ
５２…タイマーカウンタ
５３…比較部
１２１…失敗回数レジスタ
１２２…失敗回数カウンタ
１２３…比較部
１２４…メッセージ送出停止制御部
１５１…失敗回数レジスタ
１５２…失敗回数カウンタ
１５３…比較部
１５４…登録メッセージ受付拒否制御部
２０１…移動登録処理部
２０２…データ入出力部
２０３…通信処理部
２１１…ユーザ認証データベース
２１２…チャレンジ生成部
２１３…パスワード抽出部
２１４…ユーザ情報抽出部
２１５…登録応答生成部

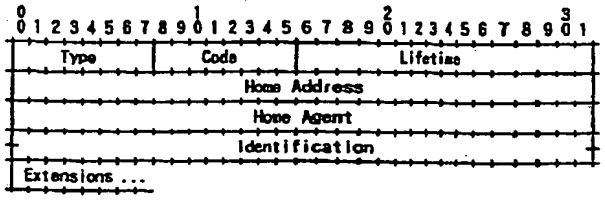
【図２】



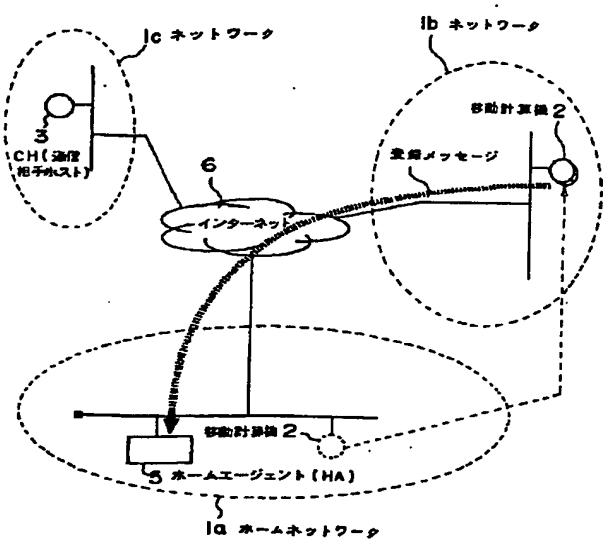
【図３】



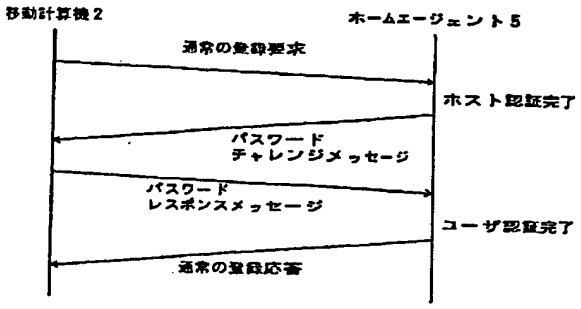
【図４】



【図1】



【図5】



【図6】

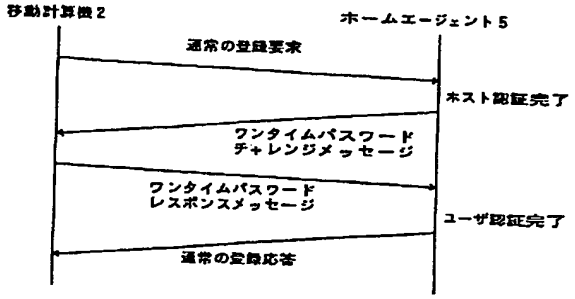
Type=137(passwd challenge)
Home address
Home agent
Identification

(a)

Type=138(passwd response)
Home address
Home agent
Identification
Password string (variable length)

(b)

【図7】



【図8】

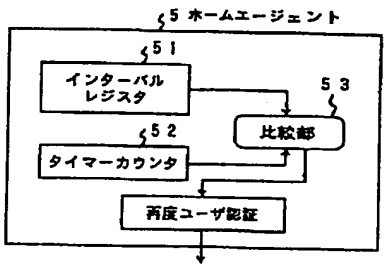
Type=139(onetime passwd challenge)
Home address
Home agent
Identification
challenge code

(a)

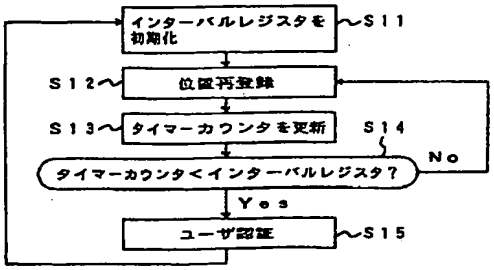
Type=140 (onetime passwd response)
Home address
Home agent
Identification
Password string (variable length)

(b)

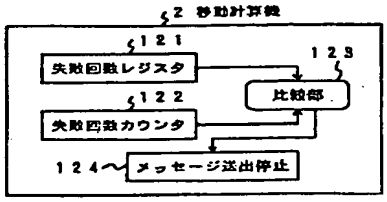
【図9】



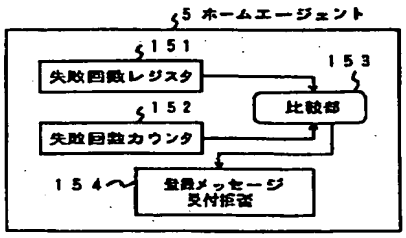
【図１０】



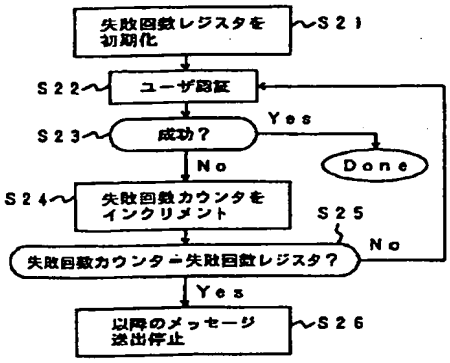
【図１１】



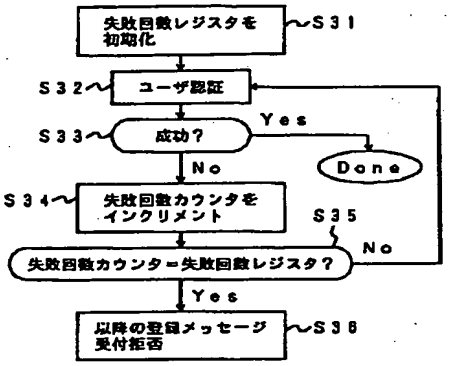
【図１３】



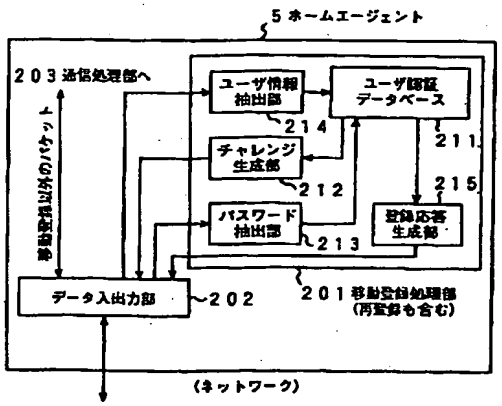
【図１２】



【図１４】



【図１５】



フロントページの続き

(51)Int.Cl.6	識別記号	FI	
H04L 12/28		H04L 11/20	B
12/66			

(72)発明者　津田　悦幸
神奈川県川崎市幸区小向東芝町1番地　株式会社東芝研究開発センター内

(72)発明者　岡本　利夫
神奈川県川崎市幸区小向東芝町1番地　株式会社東芝研究開発センター内